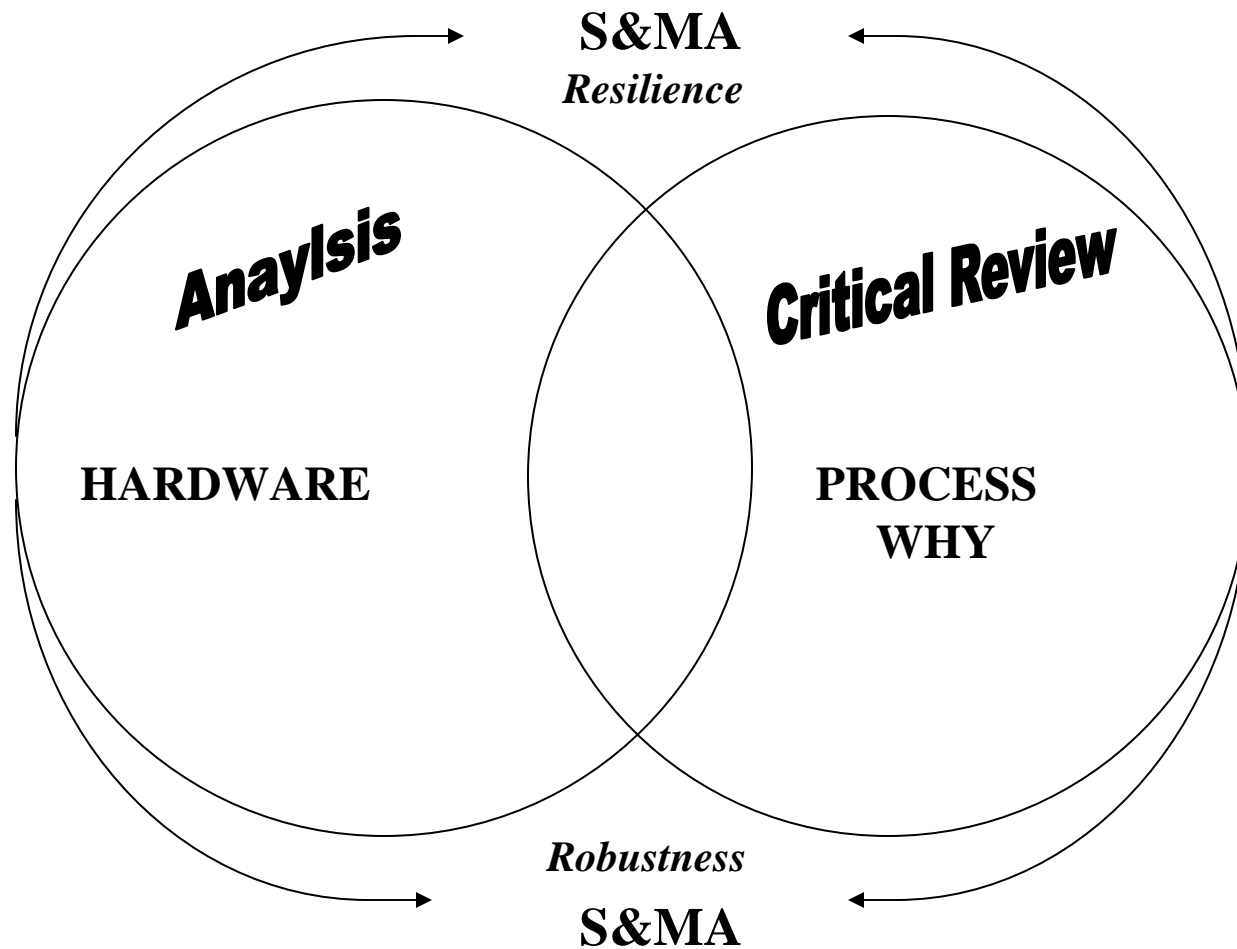


# **System Safety and Mission Assurance Contributions to Project Management**

Ronnie Goodin    KSC



**PROJECT MANAGEMENT**

# Design Process

- Diane Vaughan describing the design process in The Challenger Launch Decision
  - “What appears to work so well on paper may do so only because the designer has not imagined that the structure will be subjected to unanticipated traumas or because he has overlooked a detail that is indeed the structure’s weakest link.” p. 202

# System Safety – Critical Evaluation Contribution

CAIB Opinion (page 183)

- “The Naval Reactor Program encourages minority opinions and “bad news.”
- “Leaders continually emphasize that when no minority opinions are present, the responsibility for a thorough and **critical examination** falls to management.”
- “Alternate perspectives and critical questions are always encouraged.”
- “In practice, NASA does not appear to embrace these attitudes.”

*Plans fail for lack of counsel, but with many advisors they succeed. Solomon*

*Proverbs 15:22*

# SYSTEM SAFETY

- **System Safety** - A subset of the safety discipline that provides direct support to Project Management (PM) (Increase probability of project success through a systematic approach of hazard analysis, risk assessment, and risk management)
- *Design Process* - Design engineer works in operational and mission success space & partners with the system safety engineer who works in failure space to reduce the risk of mishaps
- **Cost** - System safety program typically represented as 5% of the estimated designer man-hours.
  - The NASA system safety effort is more because of the requirement for FTA and PRA

# **Chronological contribution of system safety to PM commencing with project initiation**

- **Safety technical requirements generation**
  - **Example sources**
    - **Lessons Learned Database**
  - **Standards and Specifications**
- **Requirements Management - Risk Mgt**
  - **MIL-STD-882 - judgment oriented based on program need - maximum flexibility**
  - **Rulebook process - non-judgment oriented, applied independent of program need - near inflexible**

# **Chronological contribution of system safety to PM commencing with project initiation**

## ***continued***

- **Development of contract requirements in the Statement of Work and for the contract data requirements (analyses & reports)**
  - **Example analyses requirements**
    - **System Safety Plan**
    - **Preliminary Hazard List**
    - **Preliminary Hazard Analysis**
    - **Operating & Support Hazard Analyses**
    - **System Hazard Analyses**
    - **Fault Tree Analyses (FTA)**
    - **Probabilistic Risk Analysis (PRA)**
- **Planning system test**
  - **Conducting test safety**
  - **Planning test to validate safety features**
- **Operation and Maintenance Planning**
  - **Examples: Source data**
    - **Operation and Support Hazard Analyses**
    - **Analyses from the Human Factors Program**  
(Human Error is involved in approximately 80% of all mishaps)

# System Safety Example

- **System safety input for a Project Manager Decision**

– LHX	.18 fatal	.34 injury
– TILT ROTOR	.18 fatal	.35 injury
– AH-64	.34 fatal	.72 injury

- (Aircrew Casualties per accident)

– LHX	4.41
– TILT ROTOR	4.35
– AH-64	5.43

- (Projected A/C losses per 100 A/C for 20 year operational life)

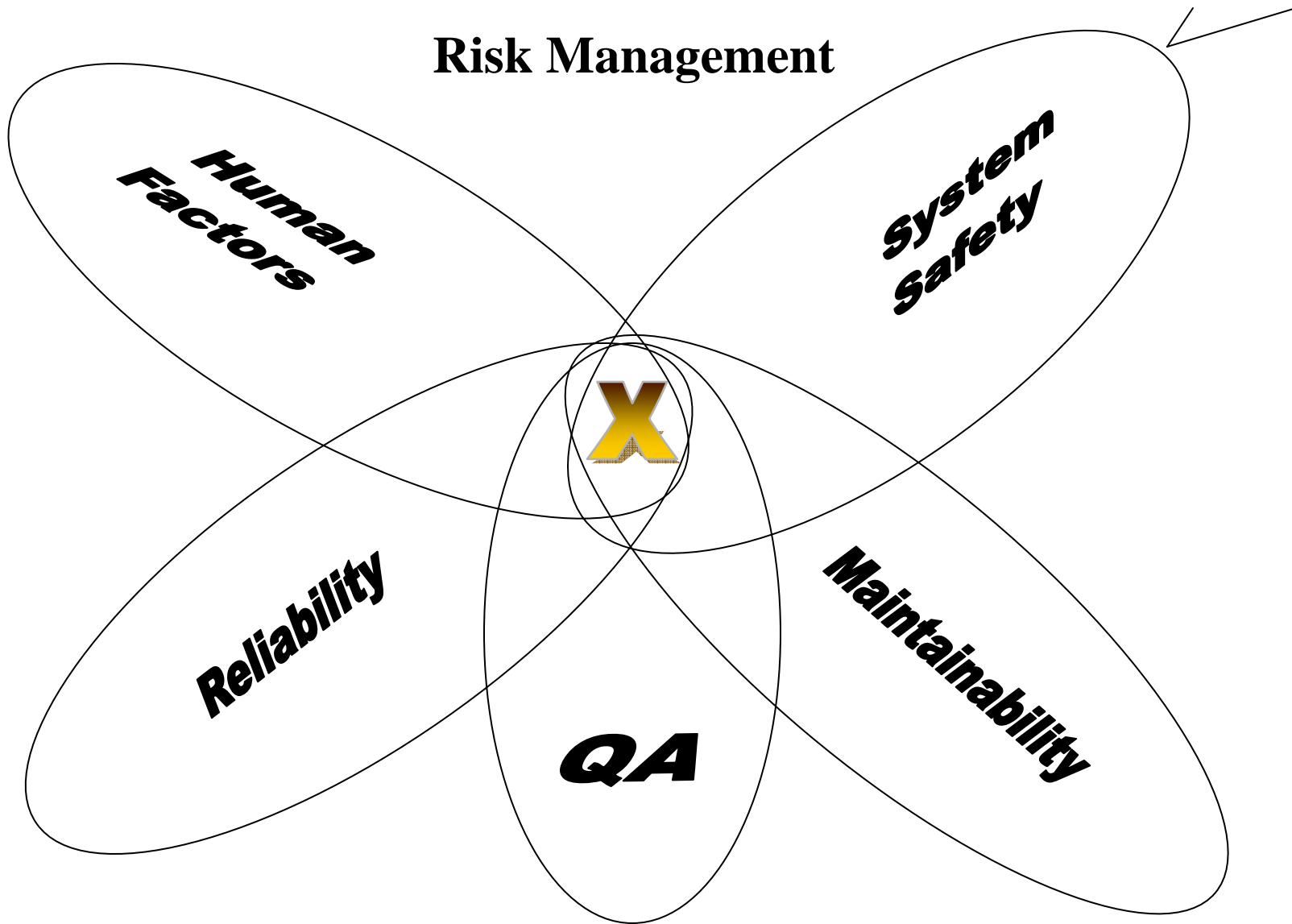


# System Safety Example

- System safety input continued
  - One engine vs. 2 engine
  - Protected tail rotor
  - Wire strike protection system
  - Rigid or articulated main rotor system
  - Crew restrain system
  - Crashworthy fuel system
  - High energy absorbing gear and fuselage

*... Of all the dangers involved in leading competitive operations, timidity is the greatest. Most of the calamities which befall an organization in competition arise from hesitation and fear of failure. - Confucius*

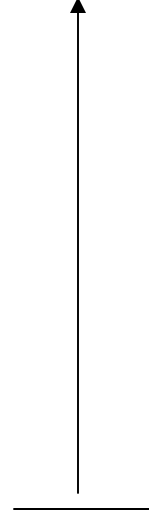
# S & MA Relationship



# QUALITY

## Quality Plan

INCREASING UNCERTAINTY

- 
- **100% inspection. (Preserve inspection records.)**
  - **Sampling, or statistical based sampling**
  - **Audits and assessments. (Preserve audit reports as a business record.)**
  - **Customer complaints**
  - **Special engineering test and processes**
    - **Non-destructive Test**
      - **National Association for Corrosion Control**

# **RELIABILITY**

**MTBF – Mean Time Between Failure**

- Failure Mode and Effect Analysis (FMEA)
- Critical Items List (CIL)

# MAINTENANCE/MAINTAINABILITY

MTBF – Mean Time To Repair

REQUIREMENT (Military & Commercial airline req. is rapid turn-around)

- Fault Detection
  - # of Maintenance personnel & training
  - Test Equipment / General purpose or Built in
  - Spare parts storage
  - Parts or module change-out
- 
- Reliability Centered Maintenance (RCM)

# **HUMAN FACTORS**

- Engineering based
- Research Psychology based

## **KHB 1700.7**

### **4.3.2.1 Electrical Requirements -**

**a. Electrical connectors shall be designed to make it physically impossible to inadvertently reverse a connection or mate the wrong connectors if a hazardous condition can be created. These connectors for energized circuits must also be of "scoop-proof" design so a partial inadvertent mismatch will not provide pin-to-pin contact.**

# SUMMARY

- “Leaders continually emphasize that when no minority opinions are present, the responsibility for a . . . critical examination falls to management.”
- Design Process - Design engineer works in success space & partners with the S&MA engineer who works in failure space to improve probability of success.